SPRING: A Strategy-Proof and Privacy Preserving Spectrum Auction Mechanism

Qianyi Huang, Yixin Tao, and Fan Wu
Shanghai Key Laboratory of Scalable Computing and Systems
Department of Computer Science and Engineering
Shanghai Jiao Tong University, China

***Abstract*—The problem of dynamic spectrum redistribution has been extensively studied in recent years. Auction is believed to be one of the most effective tools to solve this problem. A great number of strategy-proof auction mechanisms have been proposed to improve spectrum allocation efficiency by stimulating users/bidders to truthfully reveal their valuations of spectrum, which are the private information of the bidders. However, none of these approaches protect bidders' privacy. In this paper, we present SPRING, which is the first Strategy-proof and PRivacy preservING spectrum auction mechanism. We not only rigorously prove the properties of SPRING, but also extensively evaluate its performance. Our evaluation results show that SPRING achieves good spectrum redistribution efficiency with low overhead.**

I. Introduction

The fast growing wireless technology is exhausting the limited radio spectrum. Due to traditional static, expensive, and inefficient spectrum allocation by government, the utilization of radio spectrum is low in spatial and temporal dimensions. On one hand, many spectrum owners are willing to lease out or sell idle spectrum and receive proper payoff. On the other hand, many new wireless applications, starving for spectrum, would like to pay for occupying the spectrum. Therefore, redistribution of idle radio spectrum is highly important. Open markets, such as Spectrum Bridge [1], have already appeared to improve the spectrum utilization by providing services for buying, selling, and leasing idle spectrum.

Due to the fairness and allocation efficiency, auction has become a popular marketing tool to redistribute radio spectrum. In recent years, a number of strategy-proof spectrum auction mechanisms (*e.g.*, [2]–[10]) have been proposed to stimulate the bidders to truthfully bid their valuations of spectrum/channels in the auction. However, the spectrum/channel valuations are private information of the bidders. Once the valuations are revealed to the auctioneer, a corrupt auctioneer may exploit such knowledge to her advantage, either in future auctions or by reneging on the sale [11]. Therefore, privacy preservation has been regarded as a major issue in the auction design. Unfortunately, none of the existing spectrum auction mechanisms provide any guarantee on privacy preservation.

In a privacy preserving auction mechanism (*e.g.*, [11]), the outcome of the auction should be the only information that any party gains. Specifically, any party in the auction can only know the winners and their charges for winning the goods, and cannot identify any bid's submitter. However, spectrum is different from traditional goods, due to its spatial reusability, by which two spectrum users can share the same wireless channel simultaneously, if they are well-separated (*i.e.*, out of interference range of each other). Thus, existing privacy preserving auction mechanisms cannot be directly applied to spectrum auctions.

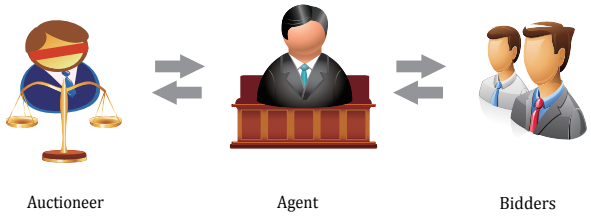


Fig. 1. Auction framework of SPRING.

In this paper, we consider the joint problem of designing both strategy-proof and privacy preserving auction mechanisms for spatial reusable goods, such as radio spectrum. We propose SPRING, which is a Strategy-proof and PRivacy preservING spectrum auction mechanism. As shown in Fig. 1, the main idea of SPRING is to separate the information known by different parties in the auction, by introducing an agent, who can interact with both the auctioneer and the bidders. The information stored at both the auctioneer and the agent is protected by cryptographic tools, such that neither of them can infer any sensitive information without the help of the other. As long as the agent and the auctioneer do not collude, SPRING can guarantee both strategy-proofness and privacy preservation.

We summarize the contributions made in this paper as follows.

- To the best of our knowledge, SPRING is the first strategy-proof and privacy preserving auction mechanisms for spectrum redistribution.
- We propose a novel and practical technique, called SPRING, to guarantee privacy preserving in a generic strategy-proof spectrum auction mechanism. The generic strategy-proof spectrum auction mechanism captures the essential idea of a category of single channel auction mechanisms, in which each bidder only requests a single channel (*e.g.*, [3], [4]).
- We also extend SPRING to adapt to the case, in which the bidders are allowed to request multiple channels, and it still achieves both strategy-proofness and privacy preservation.

- We implement SPRING and extensively evaluate its performance. Our evaluation results show that SPRING achieves good efficiency on spectrum redistribution, while inducing only a small amount of overhead.

The remainder of this paper is organized as follows. In Section II, we briefly review the related works. In Section III, we present technical preliminaries. In Section IV, we present the detailed design of SPRING for the single channel request case. In Section V, we extend SPRING to support multi-channel bids. In Section VI, we show the evaluation results of SPRING. Finally, we conclude our work and point out potential directions for future work in Section VII.

II. Related Work

Spectrum auction mechanisms have been studied extensively in recent years. A number of works were presented for market-driven dynamic spectrum auctions. For instance, [2]–[4] all are auction-based spectrum allocation mechanisms, achieving both strategy-proofness and economic-robust. Deek *et al.* proposed *Topaz* [5] to guard against time-based cheating in online spectrum auctions. Al-Ayyoub and Gupta [8] designed a polynomial-time truthful spectrum auction mechanism with a performance guarantee on revenue. Xu *et al.* [6], [7] proposed efficient spectrum allocations in multi-channel wireless networks. TAHES [9] addresses both heterogeneous spectrums and interference graph variation. Dong *et al.* [10] tackled the spectrum allocation problem in cognitive radio networks via combinatorial auction. While eliminating the overhead of strategy management, they fail to protect the privacy of bidders.

On the other hand, extensive efforts have been devoted toward privacy preserving mechanism design. In [12], differential privacy [13] was introduced as a solution concept. It shows that mechanisms with differential privacy approximate truthfulness with high probability even in the presence of collusion, arbitrary utility functions and repeated runs of the mechanism. [14] addresses efficiency and privacy tradeoffs in mechanism design and provides a general framework for analyzing the tradeoff. Brandt and Sandholm [15] investigated unconditional full privacy in sealed-bid auctions. [16]–[19] employ vast cryptography techniques to achieve security in various auction schemes. Unfortunately, these existing solutions cannot work in spectrum auctions. When applied in spectrum auctions, they either require exponential complexity, or lead to significant degradation of spectrum utilization.

III. Preliminaries

In this section, we first briefly review some important solution concepts from mechanism design, and then present our auction model together with a generic strategy-proof auction for the problem of spectrum allocation. Finally, we introduce useful tools from cryptography.

A. Solution Concepts

We briefly review the solution concepts used in this paper. A strong solution concept from mechanism design is *dominant strategy*.

Definition 1 (Dominant Strategy [20] [21])**.** *Strategy s_i is player i's dominant strategy in a game, if for any strategy $s_i' \neq s_i$ and any other players' strategy profile s_{-i}:*

$$u_i(s_i, s_{-i}) \geq u_i(s_i', s_{-i}).$$

Apparently, a dominant strategy of a player is a strategy that maximizes her utility, regardless of what strategy profile the other players choose.

The concept of dominant strategy is the basis of *incentive-compatibility*, which means that there is no incentive for any player to lie about her private information, and thus revealing truthful information is a dominant strategy for each player. A company concept is *individual-rationality*, which means that for every player participating in the game/auction is expected to gain no less utility than staying outside. We now can introduce the definition of *Strategy-Proof Mechanism.*

Definition 2 (Strategy-Proof Mechanism [22] [23])**.** *A mechanism is strategy-proof when it satisfies both incentive-compatibility and individual-rationality.*

In the field of privacy preservation, k-anonymity [24] is commonly used criteria for evaluating a privacy preserving scheme. A scheme provides k-anonymity protection when a person cannot be distinguished from at least $k-1$ individuals.

Definition 3 (k-anonymity [24])**.** *A privacy preserving scheme satisfies k-anonymity, if no party can identify a particular participant's sensitive information with probability more than $1/k$ by itself.*

In this paper, we consider the problem of privacy preserving in a semi-honest model, in which each party correctly follows the protocol specification, but attempts to infer additional information by analyzing the messages received during the execution [25]–[27].

B. Auction Model

As shown in Fig. 1, we model the process of spectrum allocation as a sealed-bid auction, in which there is an *auctioneer*, an *agent*, and a group of small service providers (*bidders*). There are a number of orthogonal and homogenous spectrum channels that can be leased out to a set of bidders, such as WiFi access points, who want to temporarily lease channels to serve their customers in particular geographic regions. In contrast to existing work on spectrum auction (*e.g.*, [2]–[4]), we have an additional trustworthy authority, called agent, who can communicate with both the auctioneer and the bidders. The bidders simultaneously submit their bids (encrypted in this paper) for channels via the agent to the auctioneer, such that no buyer can know the other participants' information. The auctioneer decides the allocation of channels and the charges for the auction winners based on the bids.

We consider that there is a set $\mathbb{C} = \{1, 2, \ldots, c\}$ of orthogonal and homogenous channels. Different from allocation of traditional goods, wireless channels can be spatially reused, meaning that more than one well-separated bidders can work

on the same channel simultaneously, if they do not interfere with each other.

We also consider that there is a set $\mathbb{N} = \{1, 2, \ldots, n\}$ of bidders. Each bidder $i \in \mathbb{N}$ requests a single channel (in Section IV) or multiple channels (in Section V), and has a valuation v_i per channel. The per channel valuation can be the revenue gained by the bidder for serving her subscribers, and is private to the bidder herself, which is known as *type* in the literature. Let $\vec{v}$ denote the valuation profile of the bidders

$$\vec{v} = (v_1, v_2, \ldots, v_n).$$

In the auction, the bidders simultaneously choose their bids, denoted by

$$\vec{b} = (b_1, b_2, \ldots, b_n),$$

which are based on their types, and submit the encrypted bids to the auctioneer via the agent.

The auctioneer determines the set of winning buyers $\mathbb{W} \subseteq \mathbb{N}$, channel allocation to the bidders $\vec{a} = (a_1, a_2, \ldots, a_n)$, and the charging profile $\vec{p} = (p_1, p_2, \ldots, p_n)$.

Then the utility u_i of bidder $i \in \mathbb{N}$ can be defined as the difference between her valuation on the channels won and the charge p_i:

$$u_i = v_i a_i - p_i.$$

We assume that the bidders are rational. The objective of each bidder is to maximize her utility and she has no preference over different outcomes with identical utility. We also assume that the bidders do not collude with each other.

In contrast to the bidders, the overall objective of the auction mechanism is to achieve good channel utilization and satisfaction ratio, while guaranteeing strategy-proofness and privacy preservation. Here, channel utilization is the average number of radios/bidders allocated to each channel; satisfaction ratio is the percentage of winning bidders in the auction.

C. Generic Strategy-Proof Spectrum Auction

In this section, we present a generic strategy-proof spectrum auction mechanism, which is general enough to capture the essence of a category of strategy-proof spectrum auction mechanisms (*e.g.*, [3], [4]). The generic spectrum auction presented here works in the case of single channel bids. In Section V, we will show how to extend it to adapt for multi-channel bids.

In the generic spectrum auction, bidders are first divided into non-conflicting groups in a bid-independent way:

$$\mathbb{G} = \{g_1, g_2, \ldots, g_m\},$$

s.t.,

$$g_j \cap g_l = \emptyset, \forall g_j, g_l \in \mathbb{G}, j \neq l$$

$$\text{and} \bigcup_{g_j \in \mathbb{G}} g_j = \mathbb{G}.$$

Then, a group bid σ_j for each group $g_j \in \mathbb{G}$ is calculated as follows.

$$\sigma_j = |g_j| \cdot \min\{b_i | i \in g_j\}.$$

All the bidder groups are ranked by their group bids in a non-increasing order with bid-independent tie breaking:

$$G' : \sigma'_1 \geq \sigma'_2 \geq \ldots \geq \sigma'_m.$$

Bidders from the top $w = \min(c, m)$ groups are winners. Each winning group is charged with σ'_{w+1} (0, if σ'_{w+1} does not exist). The charge is shared evenly among the bidders in each winning group. Formally, a bidder i from a winning group g_j is charged with price

$$p_i = \begin{cases} \sigma'_{w+1}/|g_j| & \text{if } m > c, \\ 0 & \text{otherwise.} \end{cases}$$

Essentially, the generic spectrum auction guarantees strategy-proofness, because the charge for a winner is independent of her bid. Due to limitations of space, we do not formally prove it.

Theorem 1. *The generic spectrum auction is a strategy-proof mechanism.*

D. Cryptographic Tools

In this paper, we employ three cryptographic tools, including order preserving encryption, oblivious transfer, and secure multi-party computation.

1) Order Preserving Encryption: OPES [28] is a representative scheme to encrypt numeric data while preserving the order. It enables any comparison operation to be directly applied on the encrypted data.

Intuitively, we can protect the privacy of bidders in the auction by encrypting the bids in a way that preserves the order of bids and carrying out comparison operations directly on the cipher text/value.

2) Oblivious Transfer: Oblivious Transfer (OT) [29] describes a paradigm of secret exchange between two parties, a sender and a receiver.

SPRING employs an efficient 1-out-of-z oblivious transfer (OT_z^1) of integers [30]. The receiver can access one of the z secrets from the sender, without getting any information about the remaining $z-1$ secrets, while the sender has no idea which of the z secrets was accessed. Algorithm 1 shows the pseudo-code of OT_z^1 proposed in [30], where z is a large prime, g and h are two generators of G_q, which is cyclic group of order q, and Z_q is a finite additive group of q elements. As long as $\log_g h$ is not revealed, g and h can be used repeatedly.

Algorithm 1 1-out-of-z Oblivious Transfer (OT_z^1)

Initialization:
System parameters: (g, h, G_q);
Sender's input: $s_1, s_2, \cdots, s_z \in G_q$;
Receiver's choice: $\alpha, 1 \leq \alpha \leq z$;

1: Receiver sends $y = g^r h^\alpha, r \in_R Z_q$;
2: Sender sends $c_i = (g^{k_i}, s_i(y/h^i)^{k_i}), k_i \in_R Z_q, 1 \leq i \leq z$;
3: By $c_\alpha = (d, f)$, receiver computes $s_\alpha = f/d^r$.

3) Secure Multi-Party Computation (SMC): SMC, first proposed by Yao [31], has recently become appropriate for some realistic scenarios. We employ secure multi-party comparison in SPRING to locate the lowest bid in each group, which enables a number of parties to carry out comparisons while preserving the privacy of their input.

IV. SPRING

In this section, we present SPRING, which is a strategy-proof and privacy preserving spectrum auction mechanism.

A. Design Rational

SPRING integrates cryptographic tools with the generic spectrum auction mechanism to achieve both strategy-proofness and privacy preservation. The main idea of SPRING is to separate the information known by different parties in the auction, so that no party in the auction has enough information to infer any sensitive information with confidence higher than $1/k$, while maintaining the functionality of the generic spectrum auction. We illustrate the designing challenges and our idea in this subsection.

(1) Information Separation

If there is a single central authority (auctioneer) carrying out the auction, it is inevitable that the sensitive information (*i.e.*, each particular bidder's bid) is revealed to the auctioneer. To prevent this threat, we introduce a new entity, called agent, who can tell the auctioneer the minimal amount of information necessary for deciding the winners and the charges, *i.e.*, the bidder grouping and the smallest bid in each group. Thus, although the auctioneer knows the smallest bid in a group, she does not know the bidder, to which the bid belongs. Therefore, the bidder, having the smallest bid in a group, is hidden among her company group members. However, the information should not be fully accessed by the agent to prevent sensitive information leakage. So, we apply an end-to-end asymmetric encryption scheme between the auctioneer and the bidders, so that the agent cannot decrypt the messages from the bidders.

(2) Bid Encryption

Since the auctioneer need to find the smallest bid in each bidder group without knowing the exact value of bids from the group members, we need a method to map the bids from the bidding space to another value space, while maintaining the comparison relation. We integrate the idea of order preserving encryption to enable such a mapping. However, the order preserving encryption cannot be processed by the bidders, in case that they may decrypt the bids of other bidders. So, we let the agent do the order preserving encryption before the auction. When bidding, the bidders contact the agent to get the mapped bids, using oblivious transfer, which prevents the agent from knowing which bids are chosen. Later, the agent stores collected end-to-end encrypted bidding messages, while only the auctioneer can decrypt the bidding messages, extract mapped bids, and find the smallest bid in the mapping space. The auctioneer can consult the agent to get the original value of the smallest mapped bid.

(3) Outcome Verification

Different from traditional auctions, it is not easy for bidders to verify the correctness of auction outcome in a privacy preserving auction. We adopt the idea of Secure Multi-party Computation (SMC) [31] to enable the bidders from the same group to find the smallest bid, and thus verify the auction outcome.

B. Design Details

SPRING works in four steps shown as follows.

Step 1: Initialization

Before running the spectrum auction, SPRING setups necessary system parameters. SPRING defines a set of possible bid values as

$$\beta = \{\beta_1, \beta_2, \ldots, \beta_z\},$$

in which

$$\beta_1 < \beta_2 < \ldots < \beta_z,$$

and requires that each bidder i's bid $b_i \in \beta$.

The agent maps each bid value $\beta_x \in \beta$ to γ_x, while maintaining the order, using the order preserving encryption scheme OPES.

$$\gamma_x = OPES(\beta_x),$$

$$\textit{s.t.}, \ \gamma_1 < \gamma_2 < \ldots < \gamma_z.$$

Here, $\gamma = \{\gamma_1, \gamma_2, \ldots, \gamma_z\}$ is a set of secrets of the agent. The agent also initializes the parameters of oblivious transfer by determining the large prime q and two generators of cyclic group G_q: (g, h).

SPRING employs an asymmetric key encryption scheme. Suppose that the auctioneer holds a private key Key_{priv}, and the matching public key Key_{pub} is distributed to the bidders. SPRING also employs a digital signature scheme, in which each bidder $i \in \mathbb{N}$ holds a signing key sk_i, and publishes the verification key pk_i.

Step 2: Bidding

Each bidder $i \in \mathbb{N}$ chooses a bid $b_i = \beta_x \in \beta$ according to her per channel valuation v_i, and then interacts with the agent through a 1-out-of-z oblivious transfer to receive $\hat{b}_i = \gamma_x$, which is the order-preserving-encrypted value of β_x, as follows.

- Bidder i randomly picks $r \in Z_q$, and sends
$$y = g^r h^x$$
to the agent.
- The agent replies the bidder i with $c = \{c_1, c_2, \ldots, c_z\}$, in which
$$c_l = \left(g^{k_l}, \gamma_l \left(y/h^l\right)^{k_l}\right), k_l \in_R Z_q, 1 \le l \le z.$$
- The bidder picks $c_x = (d, f)$ from c, and computes
$$\hat{b}_i = \frac{f}{d^r} = \frac{\gamma_x \left(y/h^x\right)^{k_x}}{\left(g^{k_x}\right)^r} = \frac{\gamma_x \left(g^r h^x/h^x\right)^{k_x}}{\left(g^{k_x}\right)^r} = \gamma_x.$$

Upon receiving $\hat{b}_i$, bidder i randomly picks a nonce r_i, and encrypts $\left[\hat{b}_i, r_i\right]$ using the auctioneer's public key Key_{pub}:

$$e_i = Encrypt\left(\left[\hat{b}_i, r_i\right], Key_{pub}\right),$$

where $Encrypt()$ is the asymmetric encryption function. The bidder i then submits the following tuple as a bid to the agent

$$[i, e_i, Sign(e_i, sk_i)],$$

where $Sign()$ is the signing function.

For each tuple $[i, e_i, sign_i]$ received, the agent checks its validity. If

$$Verify(e_i, sign_i, pk_i) = True,$$

where $Verify()$ is the signature verification function, the tuple is accepted. Otherwise, it is discarded.

Group ID	Bidder ID	Encrypted Bid
1	1_1,1_2,...,$1_{\|g_1\|}$	$e_{1,1}, e_{1,2}, \ldots, e_{1,\|g_1\|}$
2	2_1,2_2,..., $2_{\|g_2\|}$	$e_{2,1}, e_{2,2}, \ldots, e_{2,\|g_2\|}$
$\vdots$	$\vdots$	$\vdots$
m	m_1, m_2,..., $m_{\|g_m\|}$	$e_{m,1}, e_{m,2}, \ldots, e_{m,\|g_m\|}$

TABLE I
INFORMATION PUBLISHED BY THE AGENT.

After collecting all the bids, the agent groups the bidders in a bid-independent way, as in the generic strategy-proof spectrum auction, and publishes the grouping result and encrypted bids, as shown in Table I. To satisfy k-anonymity, we require that each of the valid bidder groups must contain at least $k+1$ bidders. In the table, bidder j_i is the ith member in group g_j, and $e_{j,1}, e_{j,2}, \ldots, e_{j,|g_j|}$ are encrypted bids from bidders in group g_j. Note that the order of $e_{j,i}$'s is irrelevant to the sequence of buyers in group g_j, which means that there is no one-to-one correspondence between $e_{j,i}$ and buyers j_i in any group.

Step 3: Opening

For each group $g_l \in \mathbb{G}$, the auctioneer decrypts the bids using her private key to get $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$:

$$\left[\hat{b}_{l,i}, r_{l,i}\right] = Decrypt\left(e_{l,i}, Key_{priv}\right), \forall i \in g_l,$$

where $Decrypt()$ is the asymmetric decryption function.

Since $\hat{b}_{l,i}$'s are computed by the order preserving encryption scheme, the smallest bid in group g_l must also result in the smallest order-preserving-encrypted bid in g_l. Therefore, the auctioneer can locate the smallest bid $\hat{b}_l^{min}$ in group g_l by finding the smallest one in $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,|g_l|}\right\}$:

$$\hat{b}_l^{min} = \min\left\{\hat{b}_{l,i} | i \in g_l\right\}.$$

Then, the auctioneer resorts to the agent to fetch the original value b_l^{min} of $\hat{b}_l^{min}$:

$$b_l^{min} = OPES^{-1}(\hat{b}_l^{min}),$$

where $OPES^{-1}()$ is the reverse function of the order preserving encryption scheme.

The auctioneer now can calculate the group bid of g_l:

$$\sigma_l = |g_l| \cdot b_l^{min}.$$

Similarly, the auctioneer calculates the group bids $\sigma_1, \sigma_2, \ldots, \sigma_m$ and sorts them in non-increasing order:

$$\sigma'_1 \geq \sigma'_2 \geq \ldots \geq \sigma'_m.$$

Same as the generic strategy-proof spectrum auction, the auction winners $\mathbb{W}$ are the bidders from first $w = \min(c, m)$ groups:

$$\mathbb{W} = \bigcup_{j=1}^{w} g'_j,$$

where g'_j is the group with jth highest group bid. In order to achieve strategy-proofness, each winning bidder group is charged with the group bid σ'_{w+1} of the $(w+1)$st group. (We set $\sigma'_{w+1} = 0$, if the $(w+1)$st group does not exist.) The charge is shared evenly among all group members, hence each buyer i in winning group g_l is charged with

$$p_i = \sigma'_{w+1}/|g_l|.$$

Besides the set of winners $\mathbb{W}$ and their charges $(p_i)_{i \in \mathbb{W}}$, the auctioneer also announces σ'_{w+1} for public verification.

Step 4: Verification

This is an optional step. Any bidder group g_l, in which the bidders doubt the outcome of the auction, can figure out the smallest encrypted bid $b^{min} = \min\{b_i | i \in g_l\}$ in the group by secure multi-party computation [31] without disclosing the exact owner of it. Then the relation between $b^{min} \cdot |g_l|$ and σ'_{w+1} can be verified.

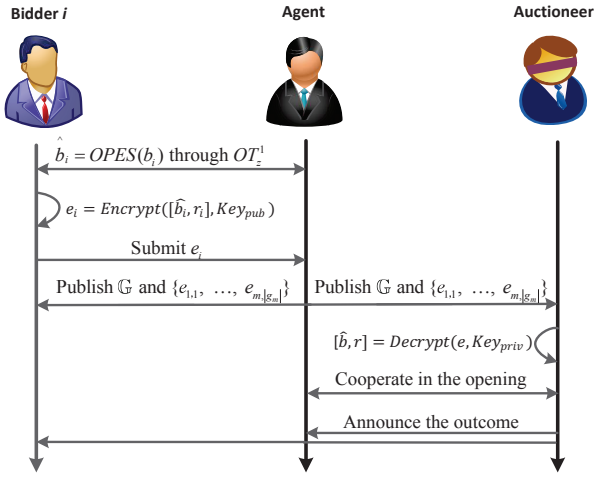


Fig. 2. Message flow.

Fig. 2 shows the message flow in SPRING.

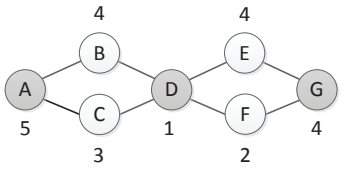


Fig. 3. Conflict graph.

C. Illustrative Example

The following example may help to illustrate our mechanism. Fig. 3 shows the interference range of seven buyers (A - G). They are competing for one channel available. Assume that $\beta = \{1, 2, 3, 4, 5\}$ and the number beside each buyer represents her bid. For clarity and simplicity, we ignore the nonce r.

In the initialization, the agent applies $OPES$ on β to get $\gamma = \{3, 7, 10, 11, 15\}$. Seven buyers interact with the agent through 1-out-of-5 oblivious transfer to receive their order-preserving-encrypted bids: $\hat{b}_A = 15, \hat{b}_B = 11, \ldots, \hat{b}_G = 11$. Then they encrypt their corresponding $\hat{b}_i$ with the auctioneer's public key Key_{pub} and submit the result e_i to the agent.

According to their conflicting conditions, seven buyers are split into two groups: $g_1 = \{A, D, G\}$, $g_2 = \{B, C, E, F\}$. The agent publishes the grouping result and encrypted bids from each group for public verification.

Group ID	Bidder ID	Encrypted Bid
1	A, D, G	e_D, e_A, e_G
2	B, C, E, F	e_E, e_F, e_B, e_C

TABLE II

The auctioneer decrypts the encrypted bids, and locates the lowest bid in each group, which turns out to be $\hat{b}_1^{min} = 3$, $\hat{b}_2^{min} = 7$. Then she resorts to the agent for the original values of $\hat{b}_1^{min}$ and $\hat{b}_2^{min}$, resulting in $b_1^{min} = 1$, $b_2^{min} = 2$. $\sigma_1 = 3 \times 1 = 3$, $\sigma_2 = 4 \times 2 = 8$, thus $\sigma_2 > \sigma_1$. Therefore, g_2 is the winning group and B, C, E, F each is charged with

$$p_{B,C,E,F} = \sigma_1/4 = 3/4.$$

D. Analysis

In this section, we show the strategy-proofness, k-anonymity, as well as some other attractive properties of SPRING.

The strategy-proofness of SPRING is inherited from the generic strategy-proof spectrum auction. Therefore, we omit the proof here and directly draw the following conclusion, due to the limitations of space.

Theorem 2. *SPRING is a strategy-proof spectrum auction mechanism.*

Next, we focus on the k-anonymity of SPRING.

Theorem 3. *SPRING guarantees k-anonymity.*

Proof: In SPRING, there are two central authorities, including the auctioneer and the agent. The auctioneer knows the smallest bid in each group, but does not know which bidder it belongs to. The agent knows the encrypted bids, but has no way to decrypt any of them. Since no other party can get even more information than the auctioneer or the agent, we focus on the privacy protection against the auctioneer and the agent in this proof.

We distinguish the following two cases:

- **Case 1:** Bidder i belongs to a bidder group g_l that is satisfied with the outcome of the auction.

  On one hand, the bidder i gets $\hat{b}_i = \gamma_x$ through 1-out-of-z oblivious transfer from the agent, who is unaware of which γ_x has been accessed by the bidder. Bidder i then sends the encrypted bid e_i to the agent, who cannot decrypt e_i without knowing the private key of the asymmetric encryption scheme. Although the agent may know the smallest bid in group g_l later when the auctioneer consults her for calculating the group bid, she still cannot infer the encrypted bid or the bidder, to which the smallest bid corresponds. So, the agent can not distinguish the smallest bid of group g_l out of at least k bidders.

  On the other hand, although the auctioneer can decrypt a ciphertext e_i to get $\hat{b}_i$, she can only reversely map the lowest $\hat{b}_{min}$ to the original bid b_{min} for each group, resorting to the agent. However, the auctioneer still cannot infer the bidder, to which b_{min} belongs out of at least k members in group g_l, since the mapping between bidder's ID and the encrypted bid is hidden by the agent.

  So, neither the agent, nor the auctioneer, can identify any bidder's bid with probability higher than $1/k$.
- **Case 2:** Bidder i belongs to a bidder group g_l, who wants to verify the auction outcome. This case only diverges from the previous one in the public verification step. Therefore, we focus on the verification step here.

  Since secure multi-party computation is applied to find the smallest b_l^{min} in group g_l, even a group member cannot distinguish the owner of b_l^{min} from the rest k bidders.

Therefore, we can conclude that SPRING guarantees k-anonymity. ■

Besides strategy-proofness and k-anonymity, SPRING also achieves the following nice properties.

- *Public Verifiability*: It enables bidder groups to verify the outcome of the auction in public verification step.
- *Non-Repudiation*: No bidder can deny her bid after the auction, since her signature is required to be verified when the bidder submits her bid to the agent.
- *Low Communication Overhead*: When z is constant, the communication overhead induced by SPRING is $\mathcal{O}(n)$, where n is the number of bidders.
- *Low Computation Overhead*: The cryptographic tools adopted by SPRING are light weighted schemes, which only induce small amount of computation overhead. Our evaluation results show that the computation overhead of SPRING is rather low.

V. Extension for Multi-Channel Bids

In the previous section, we propose a strategy-proof and privacy preserving auction mechanism, in which each bidder bids for a single channel. In this section, we extend our mechanism SPRING to adapt to the scenario, in which each bidder can bid for multiple channels. Same as before, our extension achieves both strategy-proofness and k-anonymity.

We now allow each bidder $i \in \mathbb{N}$ to demand d_i channels. Let $\vec{d}$ denote the demand profile of the bidders:

$$\vec{d} = (d_1, d_2, \ldots, d_n).$$

We assume that each bidder has identical valuation on different channels. In the auction, each bidder i submits not only her encrypted bid per channel v_i, but also the number of channels demanded d_i. We also assume that the bidders do not cheat the demands for two reasons. On one hand, the auction only allocates the channels to the bidders up to their demands. A bidder's demand definitely cannot be contented if she lowers the demand. On the other hand, over demanding may result in winning more than enough channels. Although the bidder has no valuation on the extra channels, she still need to pay for them.

To extend SPRING to adapt to multi-channel bids, we introduce *virtual group*, and update bidding and opening steps of SPRING. Note that the basic version of SPRING presented in Section IV is a special case of the extended SPRING.

A. Virtual Group

In the extended SPRING, the bidders from the same group may demand different numbers of channels. To represent the various demands in a bidder group, we introduce the concept of *virtual group*.

Given a bidder group $g_l \subseteq \mathbb{N}$, let $\hat{d}_l$ be the maximum channel demand in group g_l:

$$\hat{d}_l = \max\{d_i | i \in g_l\}.$$

A virtual group $\tilde{g}_l^j \subseteq g_l$ is the set of bidders, who demand at least j channels, in bidder group g_l:

$$\tilde{g}_l^j = \{i | i \in g_l \wedge d_i \geq j\}, 1 \leq j \leq \hat{d}_l.$$

Algorithm 2 Virtual Group Generation— vgrouping(g_l)

Input: Bidder group g_l, demand profile $\vec{d}$.
Output: Set of virtual groups G_l.

1: $G_l \leftarrow \emptyset$; $\hat{d}_l \leftarrow 0$;
2: **for all** $i \in g_l$ **do**
3: $\quad \hat{d}_l \leftarrow \max(\hat{d}_l, d_i)$;
4: **end for**
5: **for** $j \leftarrow 1, \ldots, \hat{d}_l$ **do**
6: $\quad \tilde{g}_l^j \leftarrow \{i | i \in g_l \wedge d_i \geq j\}$;
7: $\quad G_l \leftarrow G_l \cup \{\tilde{g}_l^j\}$;
8: **end for**
Return G_l;

Algorithm 2 shows the pseudo-code of virtual group generation. We find the maximum channel demand $\hat{d}_l$ in group g_l (lines 2-4), and iteratively pick the bidders demanding at least j channels to form virtual group $\tilde{g}_l^j$, which is added into the set G_l of virtual groups generated from group g_l (lines 5-8). Fig. 4 may help to better illustrate the idea of virtual group.

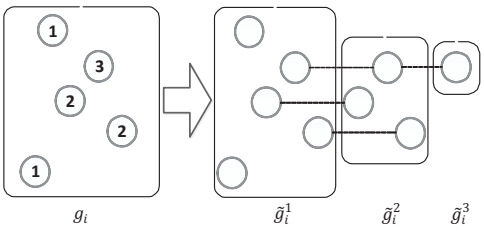


Fig. 4. A toy example.

In the extended SPRING, an original bidder group g_l is replaced by $\hat{d}_l$ virtual groups. The group bid $\tilde{\sigma}_l^j$ of virtual group $\tilde{g}_l^j$ is defined as

$$\tilde{\sigma}_l^j = \left|\tilde{g}_l^j\right| \cdot \min\{b_i | i \in g_l\}.$$

Note that the smallest bid in group g_l, instead of virtual group $\tilde{g}_l^j$, is used to calculate the group bids of virtual groups, in order to guarantee k-anonymity.

B. Extension Details

The procedures of initialization and verification are same as those in the basic SPRING. Due to limitations of space, we focus on the differences in the steps of bidding and opening.

Step 1: Initialization

Please refer to Section IV-B for details.

Step 2: Bidding

In order to include the information of channel demands, the tuple submitted by bidder i to the agent must has one more element d_i:

$$[i, e_i, d_i, Sign(e_i || d_i, sk_i)],$$

where $||$ is a concatenation operation.

The agent collects the bidding messages, verifies the validity, and publishes the grouping results and encrypted bids. This time, beside each bidder's ID, there is a corresponding channel demand, as shown in Table III.

Group ID	Bidder ID & Demand	Encrypted Bid
1	$[1_1, d_{1_1}], \ldots, [1_{\lvert g_1 \rvert}, d_{\lvert g_1 \rvert}]$	$e_{1,1}, \ldots, e_{1,\lvert g_1 \rvert}$
2	$[2_1, d_{2_1}], \ldots, [2_{\lvert g_2 \rvert}, d_{\lvert g_2 \rvert}]$	$e_{2,1}, \ldots, e_{2,\lvert g_2 \rvert}$
$\vdots$	$\vdots$	$\vdots$
m	$[m_1, d_{m_1}], \ldots, [m_{\lvert g_m \rvert}, d_{\lvert g_m \rvert}]$	$e_{m,1}, \ldots, e_{m,\lvert g_m \rvert}$

TABLE III
Information published by the agent.

Step 3: Opening

The auctioneer is informed the information of grouping and encrypted bids from Table III published by the agent, and decrypts the encrypted bids to get $\left\{\hat{b}_{l,1}, \hat{b}_{l,2}, \ldots, \hat{b}_{l,\lvert g_l \rvert}\right\}$ for

each $g_l \in \mathbb{G}$. Resorting to the agent, the auctioneer retrieves the original value of the smallest bid b_l^{min} of each $g_l \in \mathbb{G}$.

Then, the auctioneer invokes Algorithm 2 to form the virtual groups:

$$\tilde{\mathbb{G}} = \bigcup_{g_l \in \mathbb{G}} G_l.$$

For each virtual group $\tilde{g}_l^j \in \tilde{\mathbb{G}}$, the auctioneer calculates the virtual group bid:

$$\tilde{\sigma}_l^j = \left|\tilde{g}_l^j\right| \cdot b_l^{min}.$$

Next, the auctioneer sorts all the virtual groups according to their virtual group bids in non-increasing order:

$$\tilde{\sigma}_1'' \geq \tilde{\sigma}_2'' \geq \ldots \geq \tilde{\sigma}_{\sum_{g_l \in \mathbb{G}} \hat{d}_l}''.$$

The auction winners $\mathbb{W}'$ are the bidders in the first $w' = \min(c, \sum_{g_l \in \mathbb{G}} \hat{d}_l)$ virtual groups:

$$\mathbb{W}' = \bigcup_{j=1}^{w'} g_j'',$$

where g_j'' is the jth highest bid virtual group. The number of channels each winner $i \in \mathbb{W}'$ wins is

$$a_i = \sum_{1 \leq j \leq w' \wedge i \in g_j''} 1.$$

Since a bidder may be in multiple virtual groups, the previous method of charging can no longer be applied. We present a new charging method as shown by Algorithm 3.

Algorithm 3 Charging Algorithm— charging(i)

Input: Set of virtual groups $\tilde{\mathbb{G}}$ and corresponding virtual group bids $\left(\tilde{\sigma}_l^j\right)_{\tilde{g}_l^j \in \tilde{\mathbb{G}}}$, winner $i \in g_l$.
Output: Charge p_i.
1: $\tilde{\mathbb{G}}' \leftarrow \tilde{\mathbb{G}} \setminus \left\{\tilde{g}_l^j | 1 \leq j \leq \hat{d}_l\right\}$;
2: Sort the virtual groups in $\tilde{\mathbb{G}}'$ by virtual group bid in non-increasing order $\sigma_1^{\triangle} \geq \sigma_2^{\triangle} \geq \ldots \geq \sigma^{\triangle}_{\sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k}$;
3: $p_i \leftarrow 0$;
4: **for** $h \leftarrow 1, \ldots, a_i$ **do**
5: $\quad t \leftarrow \min\left(c - h + 1, \sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k\right)$;
6: $\quad$ **if** $t = c - h + 1$ **then**
7: $\quad\quad p_i \leftarrow p_i + \sigma_t^{\triangle} / |\tilde{g}_l^h|$;
8: $\quad$ **end if**
9: **end for**
Return p_i;

In Algorithm 3, we remove all the virtual groups generated from the bidder group, to which the winning bidder i belongs to, and sort the rest virtual groups by virtual group bids in non-increasing order (lines 1-2). Then, for each channel h won by bidder i, we locate the virtual group in the sorted list, after which wins a channel, bidder i cannot win channel h. If such a virtual group does not exist, then channel h is free of charge for bidder i. Otherwise, the located virtual group's bid is used to calculate the charge for bidder i on channel h. The charge on channel h is set to $\sigma_t^{\triangle} / |\tilde{g}_l^h|$. The total charge for bidder i is the sum of charges on all the channels won (lines 3-9).

Finally, the auctioneer releases the set of winners $\mathbb{W}'$, the channel allocation profile $\vec{a}$, and the charge profile $\vec{p}$.

Step 4: Verification

Please refer to Section IV-B for details.

C. Analysis

Again, we show that SPRING satisfies both strategy-proofness and k-anonymity, in the case of multi-channel bids.

Theorem 4. *SPRING is a strategy-proof spectrum auction mechanism, despite of multi-channel bids.*

Proof: We consider an arbitrary bidder $i \in g_l$ in the auction. Her utility is

$$\begin{aligned} u_i &= v_i a_i - p_i \\ &= v_i a_i - \sum_{h=1}^{a_i} p_i^h, \end{aligned}$$

where

$$p_i^h = \begin{cases} \sigma^{\triangle}_{c-h+1} / |\tilde{g}_l^h| & \text{if } \sum_{g_k \in \mathbb{G} \wedge i \notin g_k} \hat{d}_k \geq c - h + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Since p_i^h's are independent of the bidder i's bid b_i, the utility is a function on the number of allocated channels a_i.

Suppose a_i is the number of channels won by bidder i, when she bids truthfully, *i.e.*, $b_i = v_i$. We then distinguish two cases:

- The bidder i wins more channels (*i.e.*, $a_i' > a_i$) by bidding another value $b_i' \neq b_i$. This happens only when the bidder i holds the smallest bid in group g_l when bidding truthfully, and wins more channels by raising her bid (*i.e.*, $b_i' > b_i$) to increase the virtual groups' bids. Let $h (a_i < h \leq a_i')$ be the hth additional channel won by the bidder i. Then $p_i^h > 0$, because otherwise the bidder would win this channel, when bidding truthfully. The utility got on this channel is

$$\begin{aligned} u_i^h &= v_i - p_i^h \\ &= v_i - \sigma^{\triangle}_{c-h+1} / |\tilde{g}_l^h| \\ &= v_i - b_l'^{min} |\tilde{g}_l^h| / |\tilde{g}_l^h| \\ &= v_i - b_l'^{min} \\ &\leq v_i - b_i \\ &= 0. \end{aligned}$$

  Therefore, getting any more channel does not increase the bidder i's utility.
- The bidder i wins less channels (*i.e.*, $a_i' < a_i$) by bidding another value $b_i' \neq b_i$. Since the charging algorithm guarantees that

$$p_i^h \leq b_i, \forall 1 \leq h \leq a_i,$$

the utility got on the hth channel is always non-negative

$$u_i^h = v_i - p_i^h \geq v_i - b_i = 0.$$

Therefore, losing any channel cannot benefit bidder i. Consequently, bidding truthfully is every bidder's dominant strategy, and thus SPRING satisfies incentive-compatibility.

Furthermore, since any bidder who loses in the auction is free of charge, and also since any winner is charged on each channel with price not exceeding her bid, SPRING also satisfies individual-rationality.

Therefore, we can conclude that SPRING is a strategy-proof spectrum auction mechanism, despite of multi-channel bids. ■

Since SPRING does not reveal any more information to any party, in the case of multi-channel bids, we have the following theorem.

Theorem 5. *SPRING guarantees k-anonymity, despite of multi-channel bids.*

Besides strategy-proofness and k-anonymity, SPRING for multi-channel bids also has good properties, including public verifiability, non-repudiation, and low communication and computation overhead. Due to limitations of space, we do not illustrate the details again.

VI. Evaluation

We have implemented SPRING and evaluated its performance on efficiency of the spectrum auction and overheads introduced. In this section, we present our evaluation results.

A. Efficiency

In the evaluation, we measure two metrics on spectrum allocation efficiency, including channel utilization and satisfaction ratio.

- *Channel utilization*: Channel utilization is the average number of radios/bidders allocated to each channel.
- *Satisfaction ratio*: Satisfaction ratio is the percentage of bidders, who get at least one channel in the auction.

We vary the number of bidders from 50 to 500, the number of channels from 5 to 50, and the terrain area from 500 meters $\times$ 500 meters to 2000 meters $\times$ 2000 meters. In each set of evaluations, we vary a factor among bidder number, channel number, and terrain area, and fix the other two. The default/fixed value for bidder number, channel number, and terrain area, is 200, 20, and 2000 meters $\times$ 2000 meters, respectively. The bidders are randomly distributed in the terrain area, and the interference range is set to 425 meters. In the case of multi-channel demand, we randomly generate the demand of each bidder from $\{1, 2, 3, 4, 5\}$.

1) Results on Channel Utilization: Fig. 5 shows the evaluation results of SPRING on channel utilization, when bidders can bid for single channel (SPRING-SINGLE) and multiple channels (SPRING-MULTIPLE).

Fig. 5(a) shows the channel utilizations achieved by SPRING, when we fix the number of channels and the terrain area, and vary the number of bidders. Here we observe that, when the number of buyers is less than 200, the channel utilization of SPRING-SINGLE is lower than that of SPRING-MULTIPLE. This is because the channels are over supplied. When we allow the bidders to demand multiple channels, the channels can be better exploited. However, with the growth of the number of bidders, especially when the number of bidders is larger or equal to 200, the channels supplied become more and more scarce compared with the number of bidders, and the competition among the bidders become more and more intense. The introduction of virtual group makes the average (virtual) group size smaller than the single-channel bid case, and thus results in lower channel utilizations.

Fig. 5(b) shows the channel utilizations achieved by SPRING, when varying the number of channels and fixing the other two factors. When the number of channels is no more than 20, SPRING-MULTIPLE has lower channel utilization than SPRING-SINGLE, due to smaller average (virtual) group size. However, with more than 20 channels supplied, SPRING-MULTIPLE has higher channel utilization than SPRING-SINGLE, due to higher demands from the bidders.

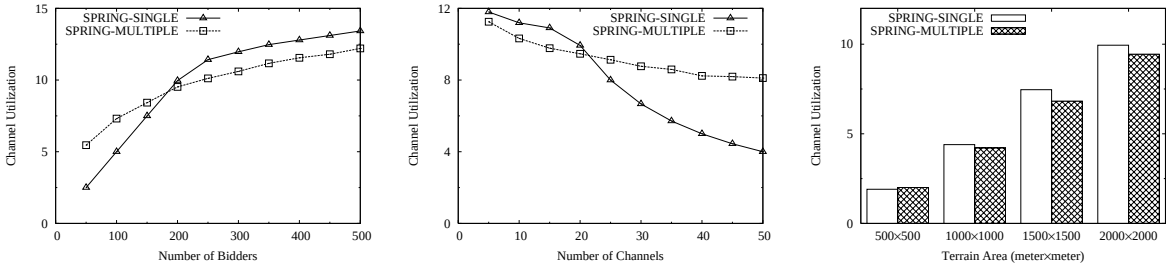
Fig. 5(c) shows the case, in which we vary the terrain area and fix the other two factors. When the terrain area is 500 meters $\times$ 500 meters or 1000 meters $\times$ 1000 meters, most of the (virtual) groups contain only 1 or 2 bidders, and thus the difference between SPRING-SINGLE and SPRING-MULTIPLE is very small. However, with the increment of terrain area, the difference on average size of (virtual) groups become larger and larger between SPRING-SINGLE and SPRING-MULTIPLE, and thus result in the channel utilization of SPRING-MULTIPLE lower than that of SPRING-SINGLE.

2) Results on Satisfaction Ratio: Fig. 6 shows the evaluation results of SPRING on satisfaction ratio.

Fig. 6(a) shows the satisfaction ratio achieved by SPRING, when varying the number of bidders and fixing the other two factors. We can see that when the number of bidders is less than 200, SPRING-SINGLE's satisfaction ratio approximates to 1, meaning that almost every bidder gets a channel in the auction. With the increasing number of bidders, satisfaction ratios of both SPRING-SINGLE and SPRING-MULTIPLE decrease as a result of more interferences. SPRING-MULTIPLE always achieves lower satisfaction ratio than SPRING-SINGLE, because SPRING-MULTIPLE allows bidders to win multiple channels, leading to the fact that more bidders cannot even obtain a single channel at all.

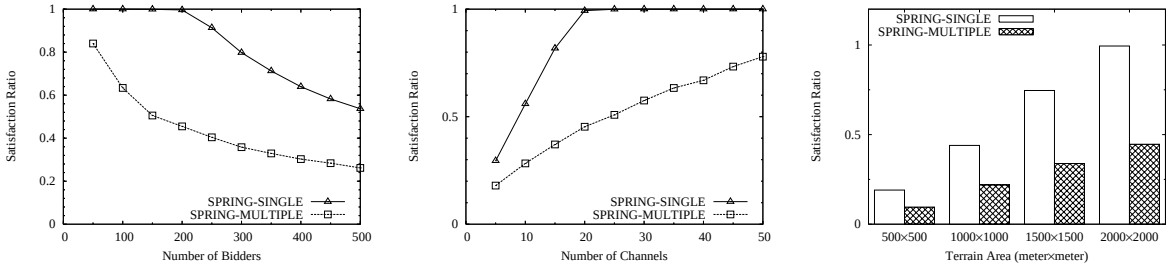
Fig. 6(b) shows the case, in which we vary the number of channels and fix the other two factors. We can see that 20 channels satisfy almost all buyers in case of SPRING-SINGLE. We also find that the satisfaction radio of SPRING-SINGLE with 10 channels is almost equal to that of SPRING-MULTIPLE with 30 channels. This is because the demands of bidders in SPRING-MULTIPLE is almost triple of that in SPRING-SINGLE, given the same number of bidders.

Fig. 6(c) shows the case, in which we vary the terrain area and fix the other two factors. Again, we can see that SPRING-SINGLE always has higher satisfaction radio than SPRING-MULTIPLE in the evaluation.



(a) Effect of number of buyers. (b) Effect of number of channels. (c) Effect of terrain area.

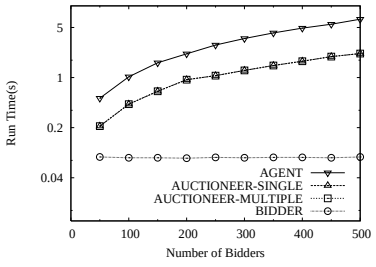
Fig. 5. Channel utilizations of SPRING, when bidders can bid for single and multiple channels.



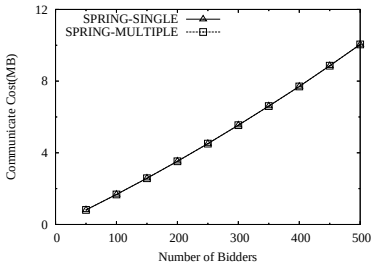
(a) Effect of number of buyers. (b) Effect of number of channels. (c) Effect of terrain area.

Fig. 6. Satisfaction ratios of SPRING, when bidders can bid for single and multiple channels.

B. Overhead



(a) Computation overhead.



(b) Communication overhead

Fig. 7. Computation and communication overheads induced by SPRING.

SPRING integrates cryptographic tools to protect bidders' privacy. A practical privacy preserving scheme should have low overheads, including computation and communication overheads, that can be afforded by wireless devices.

We implement SPRING using JavaSE-1.7 with packages java.security and javax.crypto, and use RSA with modulus of 1024 bits to do encryption/decryption and signature signing/verfication. Bidders can choose one out of 1000 predefined bids in the auction, and get 128 bits of order-preserving-encrypted value through oblivious transfer with the agent. The running environment is *Intel(R) Core(TM) i7* 2.67GHz and Windows 7.

Fig. 7(a) shows the computation overhead on the agent, the auctioneer, and each bidder, as a function of the number of bidders. We can see that the computation overhead is mainly on agent, because the agent is responsible for oblivious transfer and bidder grouping. The computation overhead of agent is about 0.515 seconds for 50 bidder, and about 6.520 seconds for 500 bidders. The auctioneer has lower computation overhead than the agent. The computation overhead on each bidder is very small.

Fig. 7(b) shows the overall communication overhead induced by SPRING. The communication overhead induced is mainly from the oblivious transfer. In the oblivious transfer, the agent needs to transfer 128 bits for each of the 100 possible bids to each bidder.

Observing the computation and communication overheads shown above, we can conclude that the overheads induced by SPRING is small enough to be applied on wireless devices.

VII. Conclusion and Future Work

In this paper, we have presented the first strategy-proof and privacy preserving auction mechanism for spectrum redistribution, namely SPRING. SPRING is good for both single-channel request and multi-channel request auctions. For both cases, we have theoretically proven the properties of SPRING. We have implemented SPRING and extensively evaluated its performance. Evaluation results have demonstrated that SPRING achieves good efficiency on spectrum redistribution, in terms of channel utilization and satisfaction radio, while inducing only a small amount of computation and communication overhead.

As for future work, one possible direction is to design a strategy-proof and privacy preserving double spectrum auction, which protects the privacy of both bidders and sellers. Another possible direction is to provide privacy preservation for combinatorial spectrum auctions.

REFERENCES

[1] Spectrum Bridge, Inc., http://www.spectrumbridge.com.

[2] X. Zhou, S. Gandhi, S. Suri, and H. Zheng, "ebay in the sky: Strategy-proof wireless spectrum auctions," in *MobiCom'08*, Sep. 2008.

[3] X. Zhou and H. Zheng, "TRUST: A general framework for truthful double spectrum auctions," in *INFOCOM'09*, Apr. 2009.

[4] F. Wu and N. Vaidya, "SMALL: A strategy-proof mechanism for radio spectrum allocation," in *INFOCOM'11*, Apr. 2011.

[5] L. B. Deek, X. Zhou, K. C. Almeroth, and H. Zheng, "To preempt or not: Tackling bid and time-based cheating in online spectrum auctions," in *INFOCOM'11*, Apr. 2011.

[6] P. Xu, X. Xu, S. Tang, and X.-Y. Li, "Truthful online spectrum allocation and auction in multi-channel wireless networks," in *INFOCOM'11*, Apr. 2011.

[7] P. Xu, X.-Y. Li, S. Tang, and J. Zhao, "Efficient and strategyproof spectrum allocations in multichannel wireless networks," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 580–593, 2011.

[8] M. Al-Ayyoub and H. Gupta, "Truthful spectrum auctions with approximate revenue," in *INFOCOM'11*, Apr. 2011.

[9] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "TAHES: Truthful double auction for heterogeneous spectrums," in *INFOCOM'12*, Mar. 2012.

[10] M. Dong, G. Sun, X. Wang, and Q. Zhang, "Combinatorial auction with time-frequency flexibility in cognitive radio networks," in *INFOCOM'12*, Mar. 2012.

[11] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *EC'99*, Oct. 1999.

[12] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *FOCS'07*, Oct. 2007.

[13] C. Dwork, "Differential privacy," in *ICALP'06*, 2006.

[14] X. Sui and C. Boutilier, "Efficiency and privacy tradeoffs in mechanism design," in *AAAI'11*, Aug. 2011.

[15] F. Brandt and T. Sandholm, "On the existence of unconditionally privacy-preserving auction protocols," *ACM Transactions on Information and System Security*, vol. 11, no. 2, pp. 6:1–6:21, May 2008.

[16] Y. F. Chung, K. H. Huang, H. H. Lee, F. Lai, and T. S. Chen, "Bidder-anonymous english auction scheme with privacy and public verifiability," *Journal of Systems and Software*, vol. 81, no. 1, pp. 113 – 119, 2008.

[17] M. Jakobsson and A. Juels, "Mix and match: Secure function evaluation via ciphertexts," in *Advances in Cryptology – ASIACRYPT 2000*, 2000, vol. 1976, pp. 162–177.

[18] K. Sako, "An auction protocol which hides bids of losers," in *Public Key Cryptography*, 2000, vol. 1751, pp. 422–432.

[19] K. Peng, C. Boyd, E. Dawson, and K. Viswanathan, "Robust, privacy protecting and publicly verifiable sealed-bid auction," in *Information and Communications Security*, 2002, vol. 2513, pp. 147–159.

[20] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. MIT Press, 1994.

[21] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.

[22] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*. Oxford Press, 1995.

[23] H. Varian, "Economic mechanism design for computerized agents," in *USENIX Workshop on Electronic Commerce*, 1995.

[24] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[25] Y. Lindell and B. Pinkas, "Privacy preserving data mining," in *Advances in Cryptology - Crypto2000*, Aug. 2000.

[26] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *SIGKDD'02*, Jul. 2002.

[27] Z. Yang, S. Zhong, and R. N. Wright, "Privacy-preserving classification of customer data without loss of accuracy," in *SDM'05*, Apr. 2005.

[28] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in *SIGMOD'04*, 2004.

[29] M. O. Rabin, "How to exchange secrets with oblivious transfer," Aiken Computation Lab, Harvard University, Tech. Rep., 1981.

[30] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Transactions on Computers*, vol. 53, no. 2, pp. 232–240, Feb. 2004.

[31] A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in *FOCS'82*, 1982.